BY ORDER OF THE COMMANDER
HQ AIR FORCE PERSONNEL CENTER

AIR FORCE PERSONNEL CENTER
INSTRUCTION 33-106

14 AUGUST 2012

Communications and Information

AFPC PRIVACY ACT (PA) PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-publishing.af.mil.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFPC/DS1

Certified by: HQ AFPC/DS
(Mr. Michael K. Gamble)

Supersedes: AFPCI33-106, 28 June 2011

Pages: 14

The purpose of this instruction is to describe Privacy Act (PA) roles, responsibilities, and requirements within the Air Force Personnel Center (AFPC). This publication carries out procedures from AFI 33-332, *Air Force Privacy Program;* 33-129, *Web Management and Internet Use;* AFI 33-119, *Air Force Messaging;* and AFI 33-200, *Information Assurance Management.* Also the Privacy Act Program references the following documentation: Department of Defense (DoD) 5400.11-R, *Department of Defense Privacy Program*, DoD Memo; *DoD Guidance on Protecting Personally Identifiable Information (PII);* Office of the Secretary of Defense (OSD) Memo 12282-05, *Notifying Individuals When Personal Information is Lost, Stolen or Compromised;* OSD Memo 15041-07, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information;* SAF/XC Memo, *Air Force Public Key Infrastructure (PKI) Policy on Encrypting and Digitally Signing E-mail Messages*.

Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847 to the AFPC Publishing Office, 550 C Street West Suite 48, Randolph AFB Texas 78150-4750, or email **afpc.publications@us.af.mil.**

Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm**.

This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by 10 U.S.C. Armed Forces; 5 U.S.C. 552a, The Privacy Act of 1974; and Air Force Instruction 33-332, Air Force Privacy Act Program. The applicable Privacy

Act SORN(s) F033 AF B, Privacy Act Request Files, and F036 AF PC Q, Personnel Data Systems (PDS) are available at **http://privacy.defense.gov/notices/usaf**/.

Vigilance must be taken to protect Personally Identifiable Information (PII) when submitting or sending nominations, applications or other documents to DoD agencies through government Internet, software applications, systems, e-mail, postal, faxing or scanning.

Refer to attachment 1 for a glossary of references and supporting information.

SUMMARY OF CHANGES

This publication is substantially revised and must be completely reviewed. This publication governs use of AFPC Form 72, *End of Day Privacy Act (PA) Checklist* and AFPC Form 73, *AFPC Privacy Act (PA) Staff Assistant Visit (SAV) Checklist*.

Chapter 1

OVERVIEW

1.1. The Privacy Act (PA).

1.1.1. Regulates collection, maintenance, use and dissemination of PII.

1.2. The purpose of the PA is to:

1.2.1. Balance government's need to maintain information about individuals with right of individuals to be protected against unwarranted invasion of their personal privacy.

1.2.2. Limits unnecessary collection of information about individuals.

1.3. Personal Information:

1.3.1. DoD 5400.11-R, *Department of Defense Privacy Program* defines Personal Information as "information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual)."

1.4. Non-Compliance Penalties:

1.4.1. As a federal employee, you are entitled to full protection and rights established by the PA. In addition to being protected by this act, federal employees who work with government records containing PII are responsible for carrying out requirements of the PA.

1.4.1.1. The importance of these responsibilities is evident from criminal penalties imposed on federal employees who violate certain sections of the law.

1.4.2. An individual may be found guilty of a misdemeanor and fined no more than $5,000 for:

1.4.2.1. Maintaining a PA system of record that has not been published in the Federal Register.

1.4.2.2. Making an unauthorized disclosure.

1.4.2.3. Obtaining access to PA information under false pretenses.

1.4.3. Injured parties may file a civil lawsuit against the AF for failing to comply with the PA.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. AFPC PA Policy Officer:

2.1.1. Provide oversight and direction to AFPC PA Office/Manager.

2.1.2. Develop AFPC PA Policy.

2.1.3. Ensure PA awareness throughout AFPC.

2.1.4. Approve AFPC PA Office/Manager publications, forms and messages recommendations.

2.1.4.1. Respond to OPR with AFPC PA Office/Manager recommendations.

2.1.5. Review AFPC PA Office/Manager Privacy Impact Assessments (PIA) recommendations prior to submission to SAF/A6PP.

2.1.6. Review AFPC PA Office/Manager System of Records Notices (SORN) recommendations prior to submission to SAF/A6PP.

2.1.7. Evaluate health of AFPC PA program.

2.1.7.1. Approve AFPC PA Office/Manager SAV recommendations/findings.

2.1.8. Provide direction to AFPC PA Office/Manager to resolve PA complaints, allegations or violations.

2.1.9. Provide direction to AFPC PA Office/Manager for full and partial denial recommendations.

2.1.10. Ensure AFPC PA Office/Manager provides annual, specialized, and PA System of Record Training.

2.1.11. Ensure quarterly update of Privacy Officials' names, office symbols, telephone numbers, fax numbers, unclassified and/or classified email addresses to SAF/A6PP for point of contact (POC) continuity.

2.1.12. Approve Quarterly Training reports, Section 803 and other reports as required and directed by SAF/A6PP.

2.1.13. Provide guidance to AFPC and tenant units to implement PA program.

2.2. AFPC PA Office/Manager. AFPC PA Office/Manager completes the following:

2.2.1. Train PA monitors (PAM).

2.2.1.1. Provide annual, specialized, and PA System of Record Training, etc.

2.2.1.2. Track PAM training (i.e., Excel spreadsheet, sign in sheet, or e-mail confirmation).

2.2.2. Promote PA awareness throughout AFPC.

2.2.2.1. Prepare and Disseminate "Did You Knows" (DYK) to PAMs.

2.2.3. Ensures accurate verbiage used in publications, forms, and messages IAW PA policies.

2.2.3.1. Publications and forms:

2.2.3.1.1. Validate SORN referenced where PII collected.

2.2.3.1.2. Vigilance statement below is applied to Publication when PII is being collected.

"Vigilance must be taken to protect Personally Identifiable Information (PII) when submitting or sending nominations, applications or other documents to DoD agencies through government Internet, software applications, systems, e-mail, postal, faxing or scanning."

2.2.3.1.3. Validate Privacy Act Statement (PAS) on "prescribed" forms.

2.2.4. Provide recommendations for PIAs.

2.2.4.1. Validate PA warning banner on IT Systems.

2.2.5. Provide recommendations for SORNs.

2.2.6. Conduct Staff Assistance Visits (SAV) annually using checklist, etc.

2.2.6.1. Post schedule on DS1F - AFPC FOIA PA SharePoint site.

2.2.6.2. Prepare SAV report within five (5) duty days of SAV.

2.2.6.3. Ensure corrective actions completed.

2.2.7. Initiate investigation of PA/PII violation or complaint investigations and report findings to AFPC/DS1 for determination of next action.

2.2.8. Report PII compromises to SAF/A6PP.

2.2.8.1. Provide description of PII compromise within 1 hour of notification to United States Computer Emergency Readiness Team (US-CERT) at **www.us-cert.gov**.

2.2.9. Process denial recommendations.

2.2.10. Provide guidance to PAMs and personnel.

2.2.11. Prepare Quarterly Training reports, Section 803, etc. as required by AFPC/DS1 and SAF/A6PP.

2.2.12. Provide guidance to AFPC and tenant units to implement PA program.

2.2.13. Submit quarterly update of Privacy Officials' names, office symbols, telephone numbers, fax numbers, unclassified and/or classified email addresses to SAF/A6PP for point of contact (POC) continuity.

2.2.14. Upon approval of AFPC PA Policy Officer, submit Quarterly Training reports, Section 803 and other reports as required and directed by SAF/A6PP.

2.3. AFPC PAM:

2.3.1. Monitor PA program within respective area and serve as liaison to AFPC PA Office/Manager.

2.3.2. Appointment Requirements:

2.3.2.1. Appointed by Director (or equivalent) in writing by letter of appointment (LOA). Sample may be found on DS1F – AFPC FOIA PA SharePoint site.

2.3.2.1.1. Multiple PAMs may be assigned based on size of organization's functional areas.

2.3.2.2. Send PA LOA containing name, rank, office symbol, duty/fax phone, and organizational e-mail address mail to: **afpc.ds1f.foia.pa@us.af.mil** within five duty days of appointment.

2.3.3. Training Requirements.

2.3.3.1. Complete initial PA training within 10 duty days of appointment and annual refresher training.

2.3.3.2. Train organizational personnel on PA compliance.

2.3.3.2.1. Provide PA annual refresher training to organizational personnel.

2.3.3.2.2. Document training via excel, etc.

2.3.4. Promote PA awareness throughout functional areas of responsibility.

2.3.4.1. Disseminate DYK to users within functional areas of responsibility.

2.3.5. PA Compromise Requirements:

2.3.5.1. Report PII compromises to AFPC/PA Office.

2.3.5.2. Assist Investigating Officer in conducting PA/PII violation or complaint investigations.

2.3.5.3. Provide incident report to AFPC PA Office/Manager within 16 hours of compromise. Template at DS1F – AFPC FOIA-PA SharePoint site.

Chapter 3

COLLECTING, PROTECTING AND DESTROYING PII

3.1. PA Warning Banners:

3.1.1. AFPC IT systems containing PII shall have a PA warning banner displayed.

3.1.2. Use following language for banner: "PRIVACY ACT INFORMATION – The information accessed through this system if FOR OFFICIAL USE ONLY and must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or penalties."

3.2. Electronic Records Management (ERM) O, R, and S Drives:

3.2.1. Official (O: Drive) and Restricted (R: Drive).

3.2.1.1. AFPC, tenant units and supported organization personnel must use appropriate access controls when placing PII on O: and R: Drives.

3.2.1.2. Use controlled passwords, group permissions and accessed based on need-to-know.

3.2.2. Shared (S: Drive).

3.2.2.1. AFPC, tenant units and supported organization personnel shall <u>not</u> store PII on S: Drive.

3.3. Personal databases and excel spreadsheets:

3.3.1. Not Authorized: Moving data from original storage area (System) to personal Excel spreadsheet or access database.

3.3.2. Developing an Excel spreadsheet, Access database or another application used for convenience is not acceptable and will not be used when information is readily available and can be retrieved from that system.

3.4. Social Rosters:

3.4.1. Directorates maintaining social rosters must obtain signed consent statement from individuals before including PII such as spouses, names, home addresses, home phones, dates of birth, anniversary dates, and similar information on social rosters shared with groups of individuals. Sample may be found on DS1F – AFPC FOIA PA SharePoint site.

3.4.2. Consent statements:

3.4.2.1. Give individual choice to consent or not consent. Consent is voluntary.

3.4.2.2. State what information is solicited.

3.4.2.3. State purpose and identify disclosure recipients.

3.4.2.4. Maintain in official file plan using AFRIMS Table 33-46, Rule 27.00, *Locator or Personnel Data*, until superseded, no longer needed or on reassignment or separation of individual.

3.5. E-mails sent from government computer to personal computer:

3.5.1. Request consent from receiver prior to sending emails containing PII from government computer to personal computers.

3.5.1.1. Send receiver the following:

"AFPC, Randolph Air Force Base (AFB) TX (insert name of your office) does not guarantee security or protection of personal information or FOR OFFICIAL USE ONLY (FOUO) when sent by e-mail between government and personal computers or when mailed, scanned, and faxed to this location. However, security and privacy measures are taken according to governing instructions, regulations, and directives to protect this information once received."

3.5.1.2. Validate e-mail address.

3.5.1.3. Contact recipient to ensure receipt.

3.6. Excel Spreadsheets Containing PII (Paper and Electronic):

3.6.1. Use following verbiage for footer or bottom of Excel spreadsheet: "The information herein is For Official Use Only (FOUO) which must be protected under the FOIA and Privacy Act, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties."

3.7. Protect PII on Printers and Facsimiles:

3.7.1. Do not leave PII on or around printers /facsimiles.

3.7.2. Private /Personal Identification number (PIN) printing instructions may be used when printers are located outside your immediate areas or numerous personnel are printing to same printer. Instructions located on DS1F – AFPC FOIA-PA SharePoint site.

3.8. AFPC Messages (e. g., Personnel Services Delivery Memorandums (PSDMs), Awards, etc.) Containing PII:

3.8.1. OPR Coordination requirements for PSDMs/Messages/Awards/etc. e-mail.

3.8.1.1. Use the following in your e-mail coordination correspondence:

1. _____ Placed on restricted (AFPERS) site with access based on need-to-know
   _____ Placed on public site (PA)

2. Contain PII? ____ Yes ____No

3.8.2. Messages, PSDMs, awards, etc. sent AF-wide.

3.8.2.1. Messages on letterhead containing PII must contain:

3.8.2.1.1. SUBJECT line: (FOUO) before subject title

3.8.2.1.2. Add following paragraphs below SUBJECT line:

3.8.2.1.2.1. "The information herein is For Official Use Only (FOUO) which must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties."

3.8.2.1.2.2. "Vigilance must be taken to protect Personally Identifiable

Information (PII) when submitting or sending nominations, applications or other documents to DoD agencies through government Internet, software applications, systems, e-mail, postal, faxing or scanning."

3.8.2.2. Messages not on letterhead containing PII must contain:

3.8.2.2.1. HEADER: "FOR OFFICIAL USE ONLY"

3.8.2.2.2. Add following paragraphs below SUBJECT line:

3.8.2.2.2.1. "Vigilance must be taken to protect Personally Identifiable Information (PII) when submitting or sending nominations, applications or other documents to DoD agencies through government Internet, software applications, systems, e-mail, postal, faxing or scanning."

3.8.2.2.2.2. FOOTER/BOTTOM: "The information herein is For Official Use Only (FOUO) which must be protected under the Freedom of Information Act of 1966 and Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties."

3.9. During Business Hours:

3.9.1. Take reasonable steps to minimize risk of access of PII by unauthorized personnel.

3.9.2. Cover PII using AF Form 3227, *Privacy Act Cover Sheet* or DD Form 2923, *Privacy Act Data Cover Sheet* or place PII in drawer, cabinet, etc.

3.10. After Business Hours:

3.10.1. End of Day PA Checks. Establish PA checks to ensure PII is secured.

3.10.1.1. AFPC Form 72, *End of Day PA Checklist* may be used to ensure PII is secured.

3.10.1.2. AFPC Form 72, *End of Day PA Checklist* may be required by areas where PII incidents occur.

3.10.1.3. Completed AFPC Form 72 is maintained in official file plan using AFRIMS Table 33-45, Rule 01.00, *Office Administrative Files and Schedule of Daily Activities,* and destroyed after two years.

3.10.2. Secured buildings: Store PII in unlocked containers, desks or cabinets.

3.10.3. Unsecured buildings: Store PII in locked desks, cabinets, book cases, or locked rooms.

3.11. Transporting PII Outside AFPC Controlled Areas. PA/PII (in any media format) removal and/or transport is restricted beyond AFPC.

3.11.1. AFPC members are prohibited from downloading or storing PII with intent to transport data beyond AFPC premises using:

3.11.1.1. Personal or government-issued laptops.

3.11.1.2. Personal digital assistant (PDA).

3.11.1.3. Universal Serial Bus (USB)-type mobile storage devices.

3.11.1.4. Compact Discs (CD), Digital Versatile Discs (DVD) or any other mobile storage devices.

3.11.1.5. AFPC, tenant units and supported organizational personnel utilize remote virtual private network (VPN) methods to access PII beyond AFPC premises.

3.11.2. Authorized PII transport and removal: To meet critical mission needs requiring transporting PII in any media format beyond AFPC premises.

3.11.2.1. Transport data off-site for purpose of back-up and recovery operations.

3.11.2.2. Transport records to off-site storage.

3.11.2.3. Recall rosters.

3.11.3. Safeguards: Encrypt all electronic data transported outside AFPC premises using a product certified IAW Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*.

3.11.4. Action Officer/OPR:

3.11.4.1. Complete PII transport authorization memorandum template on DS1F – AFPC FOIA PA SharePoint site.

3.11.4.2. Obtain AFPC/CC or AFPC/CD authorization/approval to transport PII/PA.

3.12. Destruction of Paper Products:

3.12.1. Do not put documents containing PII in trash cans.

3.12.2. Do not place PII in recycling containers located under desks.

3.12.3. Place PII in secured recycle Blue/Gray bins.

3.13. Recycle (Blue/Gray) Bins:

3.13.1. Must be secured using tie tab or lock.

3.13.2. Must be sent for recycling when full. AFPC Facilities posts schedule on fence outside AFPC postal area and found on AFPC DSF SharePoint site.

3.13.3. Must not be left unsecured while waiting for pick up by contactor.

Chapter 4

COMPROMISES

4.1. Reporting:

4.1.1. AFPC and tenant units are responsible for reporting PII loss, theft or compromise.

4.1.1.1. Notify your supervisor and PAM immediately who in-turn notifies AFPC PA Office/Manager.

4.2. Use detailed instructions (available on DS1F – AFPC FOIA PA SharePoint site) for processing incidents or breaches.

4.3. Director of affected office will:

4.3.1. Appoint Investigating Officer (IO). Sample may be found on DS1F – AFPC FOIA PA SharePoint site.

4.3.2. Notify AFPC Commander of compromise.

ALFRED J. STEWART, Maj Gen, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 33-119, *Air Force Messaging,* 24 January 2005

AFI 33-129, *Transmission of Information Via the Internet,* 3 February 2005

AFI 33-200, *Information Assurance Management,* 23 December 2008

AFI 33-332, *Air Force Privacy Program,* 16 May 2011

AFI 33-360, *Publications and Forms Management,* 18 May 2006

AFMAN 33-363, *Management of Records,* 1 March 2008

Air Force Records Information Management System (AFRIMS)

Air Force Visual 33-276, *Privacy Act Label,* 1 August 2000

Directive-Type Memorandum (DTM) 07-015-USD (P&R), *DoD Social Security Number (SSN) Reduction Plan*

DoD 5200.1-R, *Information Security Program,* 14 January 1997

DoD 5400.7-R/AFMAN 33-302, *DoD Freedom of Information Act Program*, 21 October 2010

DoD 5400.11- R, *DoD Privacy Program*, 14 May 2007

DoD 6025.18R, *DoD Health Information Privacy Regulation*, 24 January 2003

DoD 5100.3, *Support of the Headquarters of Combatant and Subordinate*

Joint Commands, 24 March 2004

DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance,* 23 February 2009

DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003

Federal Information Processing Standard (FIPS) 140-2, *Security Requirements For Cryptographic Modules,* 25 May 2001

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems,* 1 February 2004

DoD Memo, *DoD Guidance on Protecting Personally Identifiable Information (PII),* 18 August 2006

OSD Memo 12282-05, *Notifying Individuals When Personal Information is Lost, Stolen or Compromised,* 15 July 2005

OSD MEMO 15041-07, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* 21 September 2007

SAF/XC Memo, *Air Force Public Key Infrastructure (PKI) Policy on Encrypting and Digitally Signing E-mail Messages,* 15 February 2007

Prescribed Forms

AFPC Form 72, *End of Day Privacy Act (PA) Checklist*

AFPC Form 73, *AFPC PA SAV Checklist*

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 3227, *Privacy Act Cover Sheet*

DD Form 2923, *Privacy Act Data Cover Sheet*

Abbreviations and Acronyms

AFPC—Air Force Personnel Center

AFRIMS—Air Force Records Information Management System

CoP—Community of Practice

CRM—Customer Relations Management

DoD—Department of Defense

DYK—Did You Know

FARM—Functional Area Records Manager

FIPS—Federal Information Processing Standards

FOUO—For Official Use Only

LOA—Letter of Appointment

OPR—Office of Primary Responsibility

OSD—Office of the Secretary of Defense

PA—Privacy Act

PAM—Privacy Act Monitor

PAS—Privacy Act Statement

PDA—Personal digital assistant

PIA—Privacy Impact Assessments

PII—Personally Identifiable Information

PIN—Personal Identification number

PKI—Public Key Infrastructure

RC—Records Custodian

RDS—Records Disposition Schedule

SAV—Staff Assistance Visit

SORN—System of Record Notices

TMT—Tracking Management Tool

SSN—Social Security Number

US-CERT—United States Computer Emergency Readiness Team

USB—Universal Serial Bus

VPN—Virtual Private Network